State of Alaska
Department of Administration

IRIS Access Affidavit

Questions? Contact DOA.DOF.IRIS.SWAT@alaska.gov

Please Print or Type

USER INFORMATION

AGENCY	EMPL ID NUM	EMPL NAME	EMPL PCN	EMPL USER ID

IRIS ENVIRONMENT REQUESTED

☐ IRIS Financial/Procurement ☐ IRIS Human Resource Management (HRM)

GENERAL INFORMATION

This form will give the employee ***VIEW ONLY*** access to IRIS. If additional security is needed, please complete and sign the IRIS Security Request Form located at:

http://doa.alaska.gov/dof/forms/resource/IRIS-Security.xlsm

ETHICAL STANDARD

I acknowledge that reasonable use and common sense must prevail in the workplace use of Office Technologies and that I must understand and comply with applicable Alaska Statute (AS), policies, and Alaska Administrative Code. The Executive Branch Ethics Act states a public employee may not "use state time, property, equipment, or other facilities to benefit personal or financial interests" (AS 39.52.120(b)(3)). Further, "standards of ethical conduct for members of the executive branch need to distinguish between those minor and inconsequential conflicts ... and those conflicts of interests that are substantial and material." (AS 39.52.110(a)(3)).

AS 11.46.740 Criminal use of computer. (a) A person commits the offense of criminal use of a computer if, having no right to do so or any reasonable ground to believe the person has such a right, the person knowingly (1) accesses, causes to be accessed, or exceeds the person's authorized access to a computer, computer system, computer program, computer network, or any part of a computer system or network, and, as a result of or in the course of that access, (A) obtains information concerning a person; (B) introduces false information into a computer, computer system, computer program, or computer network with the intent to damage or enhance the data record or the financial reputation of a person; (C) introduces false information into a computer, computer system, computer program, or computer network and, with criminal negligence, damages or enhances the data record or the financial reputation of a person; (D) obtains proprietary information of another person; (E) obtains information that is only available to the public for a fee; (F) introduces instructions, a computer program, or other information that tampers with, disrupts, disables, or destroys a computer, computer system, computer program, computer network, or any part of a computer system or network; or (G) encrypts or decrypts data. (b) In this section, "proprietary information" means scientific, technical, or commercial information, including a design, process, procedure, customer list, supplier list, or customer records that the holder of the information has not made available to the public. (c) Criminal use of a computer is a class C felony.

CRIMINAL ACTIVITY

I acknowledge that misuse of computing resources is a criminal activity under AS 11.46.484. Criminal mischief in the fourth degree. (a) A person commits the crime of criminal mischief in the fourth degree if, having no right to do so or any reasonable ground to believe the person has such a right: (3) the person knowingly accesses a computer, computer system, computer program, computer network, or part of a computer system or network. (b) Criminal mischief in the fourth degree is a class A misdemeanor.

PASSWORD CONFIDENTIALITY

I acknowledge that this account shall be used solely in the performance of my authorized job functions by the signed requestor below. I also acknowledge that I will take the necessary precautions to maintain the confidentiality of my logon ID and password; and that I will immediately report its disclosure or use by anyone other than myself to my supervisor.

This form is continued on next page.

State of Alaska
Department of Administration

IRIS Access Affidavit

Questions? Contact DOA.DOF.IRIS.SWAT@alaska.gov

Please Print or Type

USER INFORMATION

AGENCY	EMPL ID NUM	EMPL NAME	EMPL PCN	EMPL USER ID

DATA CONFIDENTIALITY

I acknowledge that I have read and understand AS 11.56.860 and AS 39.25.080. I will only access confidential information necessitated by the performance of my job functions and will not discuss, disclose, or cause disclosure of any such confidential information to anyone who does not have a business need and a legal right to know the information.

AS 11.56.860. Misuse of confidential information. (a) A person who is or has been a public servant commits the crime of misuse of confidential information if the person, (1) learns confidential information through employment as a public servant; and (2) while in office or after leaving office, uses the confidential information for personal gain or in a manner not connected with the performance of official duties other than by giving sworn testimony or evidence in a legal proceeding in conformity with a court order. (b) As used in this section, "confidential information" means information which has been classified confidential by law. (c) Misuse of confidential information is a class A misdemeanor.

AS 39.25.080. Personnel records confidential; exceptions. (a) State personnel records, including employment applications and examination and other assessment materials, are confidential and are not open to public inspection except as provided in this section. (b) The following information is available for public inspection, subject to reasonable regulations on the time and manner of inspection: (1) the names and position titles of all state employees; (2) the position held by a state employee; (3) prior positions held by a state employee; (4) whether a state employee is in the classified, partially exempt, or exempt service; (5) the dates of appointment and separation of a state employee; (6) the compensation authorized for a state employee; and (7) whether a state employee has been dismissed or disciplined for a violation of AS 39.25.160(l) (interference or failure to cooperate with the Legislative Budget and Audit Committee).

CERTIFICATION

I have read the below statutes that pertain to the certifying function. I understand that my access to IRIS HRM might include the functions of a certifying officer and if they do I accept the duties and responsibilities for the transactions and departments included.

AS 11.56.210. Unsworn falsification. (a) A person commits the crime of unsworn falsification if, with the intent to mislead a public servant in the performance of a duty, the person submits a false written or recorded statement which the person does not believe to be true (1)in an application for a benefit; or (2)on a form bearing notice, authorized by law, that false statements made in it are punishable. (b)Unsworn falsification is a class A misdemeanor. (§6 ch 166 SLA 1978).

AS 37.10.010. Disbursements. The Department of Administration shall (1) disburse money only upon vouchers certified by the department, establishment, or agency concerned, or an officer or employee of it authorized in writing to certify the vouchers; (2) make an examination of vouchers necessary to ascertain whether they are in proper form, certified and approved, computed on the basis of the facts certified; and (3) be held accountable accordingly. (§12-3-1 ACLA 1949).

AS 37.10.020. Vouchers to be approved by administrative officer. A voucher arising from the conduct of an office or administration of the state shall be approved by the administrative officer before reference to the Department of Administration for payment. (§12-3-2 ACLA 1949).

AS 37.10.030. Responsibility of officer or employee approving or certifying voucher. (a) The officer or employee approving or certifying a voucher (1)is responsible for the existence and correctness of the facts recited in the certificate or stated on the voucher or its supporting papers and for the legality of the proposed payment under the appropriation or fund involved; (2)shall give bond in the form and manner prescribed by AS 39.15 to the state, and approved by the Department of Administration, in an amount fixed by the head of the department, agency, or establishment concerned, under standards prescribed by the Department of Administration; the premium on the bond shall be paid from funds made available for the administrative costs of the department, agency, or establishment concerned; officers already bonded under other provisions of law for the faithful performance of their duties are not required to give additional bond; and (3)shall be held accountable for and required to make good to the state the amount of an illegal, improper, or incorrect payment resulting from a false, inaccurate, or misleading certificate made by the officer or employee, or a payment prohibited by law or which does not represent a legal obligation under the appropriation or fund involved.(b)In (a) of this section, an approval or certification of a voucher is effective when an authorized person uses a password assigned by the department if the certification or the voucher itself is prepared and recorded by using an electronic accounting device that is a part of the computerized state accounting systems. (§12-3-3 ACLA 1949; am §3 ch 51 SLA 1985).

AS 37.10.040. Enforcement of liability. The liability of a certifying officer or employee is enforced in the same manner as provided by law with respect to enforcement of the liability of a disbursing and other accountable officer. (§12-3-4 ACLA 1949).

State of Alaska
Department of Administration

IRIS Access Affidavit

Questions? Contact DOA.DOF.IRIS.SWAT@alaska.gov

Please Print or Type

USER INFORMATION

AGENCY	EMPL ID NUM	EMPL NAME	EMPL PCN	EMPL USER ID

IRIS ENVIRONMENT REQUESTED

☐ IRIS Financial/Procurement ☐ IRIS Human Resource Management (HRM)

SECURITY POLICY COMPLIANCE

I acknowledge that this account shall be used solely in the performance of my authorized job functions. I also acknowledge that it is my sole responsibility to ensure any use or access is compliant with the state security policies and will take all the necessary steps to ensure compliance. Security Policies are located at the following URL: http://security.alaska.gov

COMPROMISE RESOLUTION / SECURITY VIOLATIONS

Should security monitoring determine your authenticated LOGONID is compromised with malicious software, running a prohibited file-sharing program, or otherwise in violation of security policy, your LOGONID may be immediately deactivated. Reinstatement of the ID will take place only after remediation/investigation has taken place per state policy/operating procedure. Permanent account revocation could be applied depending on the severity of the offense.

SIGNATURES

Employee

Signatures acknowledges that I have reviewed and understand the following sections of this document:

- GENERAL INFORMATION,
- ETHICAL STANDARD (including AS 39.52.120(b)(3), AS 39.52.110(a)(3), and AS 11.46.740),
- CRIMINAL ACTIVITY (including AS 11.46.484),
- PASSWORD CONFIDENTIALITY,
- DATA CONFIDENTIALITY (including AS 11.56.860 and AS 39.25.080)
- CERTIFICATION (including AS 11.56.210, AS 37.10.010, AS 37.10.020, AS 37.10.030, and AS 37.10.040)
- SECURITY POLICY COMPLIANCE, and
- COMPROMISE RESOLUTION / SECURITY VIOLATIONS

PRINTED NAME	SIGNATURE	DATE
		03/24/2017

Agency Appointing Authority / Security Contact Approval

PRINTED NAME	SIGNATURE	DATE

Submit this form to:

Email: *DOA.DOF.IRIS.SWAT@alaska.gov*
Fax: (907) 465-2169

NOTE: For file retention, DOA-DOF IRIS Security Team may only retain Page 3 of this document in their files. Pages 1 and 2 language will be retained in a file copy of versions of this form.